Title (en)

DETECTION AND IDENTIFICATION OF TARGETED ATTACKS ON A COMPUTING SYSTEM

Title (de)

ERKENNUNG UND IDENTIFIZIERUNG GEZIELTER ANGRIFFE AUF EIN RECHNERSYSTEM

Title (fr)

DÉTECTION ET IDENTIFICATION D'ATTAQUES CIBLÉES D'UN SYSTÈME INFORMATIQUE

Publication

EP 4006762 B1 20230329 (EN)

Application

EP 22153459 A 20180625

Priority

- US 201762561966 P 20170922
- US 201815874983 A 20180119
- EP 18742640 A 20180625
- US 2018039220 W 20180625

Abstract (en)

[origin: US2019098040A1] Malicious activity data is obtained, that is indicative of attempted attacks on a computing system. Clusters of targets are identified and it is determined whether the malicious activity preferentially targets one cluster of targets over other. Also, low prevalence attacks are identified and it is determined whether a low prevalence attack has a high concentration in one or more of the target clusters. If the malicious activity either preferentially targets a cluster, or a low prevalence attack has a high concentration in a cluster, then the attack is identified as a targeted attack, so that remediation steps can be taken.

IPC 8 full level

G06F 21/55 (2013.01); **G06F 21/56** (2013.01); **G06F 21/57** (2013.01); **H04L 9/40** (2022.01)

CPC (source: CN EP US)

G06F 21/55 (2013.01 - EP US); **G06F 21/552** (2013.01 - CN); **G06F 21/56** (2013.01 - EP US); **G06F 21/566** (2013.01 - CN EP US); **G06F 21/577** (2013.01 - CN EP US); **H04L 63/0236** (2013.01 - CN EP US); **H04L 63/14** (2013.01 - CN EP US); **H04L 63/1416** (2013.01 - CN EP US); **H04L 63/1425** (2013.01 - CN EP US); **H04L 63/1441** (2013.01 - CN EP US)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

US 10715545 B2 20200714; **US 2019098040 A1 20190328**; CN 111108496 A 20200505; CN 111108496 B 20231103; CN 117424734 A 20240119; EP 3685295 A1 20200729; EP 3685295 B1 20220316; EP 4006762 A1 20220601; EP 4006762 B1 20230329; US 11025665 B2 20210601; US 2020304538 A1 20200924; WO 2019060014 A1 20190328

DOCDB simple family (application)

US 201815874983 A 20180119; CN 201880060963 A 20180625; CN 202311385040 A 20180625; EP 18742640 A 20180625; EP 22153459 A 20180625; US 2018039220 W 20180625; US 202016895608 A 20200608